REMARKS

Claims 1, 3-10, and 12-33 are pending. By this Amendment, claims 1, 3-5, 8-10, 14, 17, and 19 are amended. No new matter is added. Reconsideration of the application is respectfully requested.

Entry of the amendments is proper under 37 CFR §1.116 since the amendments: (a) place the application in condition for allowance (for the reasons discussed herein); (b) do not raise any new issue requiring further search and/or consideration since the amendments merely clarify the claim language and correct informalities; (c) do not present any additional claims without canceling a corresponding number of finally rejected claims; and (d) place the application in better form for appeal, should an appeal be necessary. The amendments are necessary and were not earlier presented because they are made in response to arguments raised in the final rejection. Entry of the amendments is thus respectfully requested.

Claims 1, 3-10 and 12-33 are amended merely to correct informalities and to clarify the claim language, such as first data, second data, third data, and fourth data.

The Office Action rejects claims 1, 3-10, and 12-32 under 35 U.S.C. §103(a) over U.S. Patent No. 5,502,766 to Boebert et al. (Boebert) in view of U.S. Patent No. 6,496,928 to Deo et al. (Deo). This rejection is respectfully traversed.

Applicants thank Examiners Lanier and Barron for their consideration of a personal interview. Applicants believe that the Office Action is unclear, making it difficult to understand the Examiner's intended interpretation of the applied references. Applicants' arguments below are based on their best understanding of the Office Action and the applied references. If Applicants' understanding is not correct with respect to the Examiner's intended interpretation, the Examiner is earnestly requested to contact Applicants' representative to explain his interpretation before further acting on the application.

By citing column 10, lines 22-34 and column 13, lines 42-57 of Boebert, the Office Action alleges that Boebert's storage search logic 72 in the security server 24 and the personal keying device 30 correspond to the claimed data-for-main-checking memory unit and the data-for-secondary-checking memory unit, respectively. In addition, by citing column 10, lines 22-34, the Office Action asserts that the user's ID and PIN stored in the memory of the personal keying device 30 is used to generate an encryption key.

The only portion of Boebert cited by the Examiner that teaches the use of the user's ID and PIN to generate an encrypting key (a combined key 44) is described in column 13, lines 49-51, and shown in Fig. 12. Boebert teaches that a media key/access vector pair 91 is enciphered with the combined key 44 consisting of the user's ID 48 and PIN 50 and the enclave key 40. As such, according to Fig. 12, Applicants understand that the Office Action is alleging that the key management crypt 70 corresponds to the encrypting key generation unit recited in claim 1.

Furthermore, because the cited section relates to "Media Initialization and Key Generation" (see column 12, line 16 - column 14, line 12 and Figs. 7-13), it is understood that the Office Action is applying this specific process to allegedly read on the claims.

Claim 1 recites, *inter alia*, that an encryptor encrypts data stored in the data-for-main-checking memory unit with the encrypting key generated by the encrypting key generation unit.

The Office Action states that column 13, lines 42-57 of Boebert describes that the generated encryption key is used to encrypt the access vector and media key that is stored in the storage search logic, and asserts that this passage teaches the above-described feature. However, as shown in Fig. 12 and described in column 13, lines 53-54, the enciphered packet 92 containing the media key 42 and access vector 52 is sent to the storage search logic 72 to store the enciphered packet 92 in the crypto key data base 84. Boebert does not teach or suggest that the storage search logic 72 has any capability of storing data.

Moreover, as described in column 13, lines 34-45, the access vector 52 is computed by the security policy logic 86, and the media key 42 is generated by the key management crypto 70. Therefore, Applicants respectfully submit that Boebert does not teach or suggest that the enciphered vector access and media key are stored in the storage search logic 72. Deo does not overcome this deficiency.

Thus, the asserted combination of Boebert and Deo fails to teach or suggest that the encryption encrypts data stored in the data-for-main checking memory unit with the encrypting key generated by the encrypting key generation unit as recited in claim 1. At least for this reason, Applicants respectfully submit that claim 1 is patentable over the applied prior art.

Claims 3-8 are patentable at least for their dependence on claim 1, as well as for the additional features they recite.

Claim 9 recites, *inter alia*, that second data stored in a memory unit is encrypted with the encrypting key.

First, Applicants respectfully assert that the Office Action does not identify what in Boebert or Deo allegedly corresponds to the first data and the second data. From Applicants' interpretation of the rejection applied to claim 1, Applicants understand that the user's ID and PIN allegedly correspond to the first data, and the media key and the access vector allegedly correspond to the second data. Therefore, as described above in connection with the rejection of claim 1, Applicants respectfully assert that the media key and the access vector are not stored in a memory unit. Deo does not overcome this deficiency. As such, Applicants respectfully submit that claim 9 is also patentable over the applied art.

Claim 10 recites, *inter alia*, that a decrypting key generation unit generates a decrypting key from data stored in the data-for-secondary-checking memory.

Applicants respectfully submit that the Office Action is again unclear as to which elements of the applied references allegedly correspond to these features. The Office Action describes how the user is identified as an authorized user to use a media containing an appropriate media key and asserts that such process meets the limitations of the data verification between the units, by referring to column 13, line 64 - column 14, line 13. Thus, Applicants understand that the Office Action intends to assert that Boebert teaches the claimed invention in this cited section of Boebert.

However, this cited section does not teach or suggest that the enciphered media key/access vector pair packet 92 is decrypted. In addition, the cited section does not teach or suggest any decrypting keys to decrypt the enciphered media key/access vector pair packet 92. The only teaching with respect to the enciphered media key/access vector pair packet 92 is that it is stored in the personal keying device 30.

Boebert, however, does teach in the "Media Initialization and Key Generation" section that the user's ID is decrypted by an enclave key 40 (see column 12, lines 57-60) and that the encrypted packet 90 containing the user's ID and PIN and a request is decrypted using a copy of the enclave key 40. In both cases, the enclave key 40 is used to decrypt data, but the enclave key 40 is not generated from any data. As defined in column 9, lines 63-67, the enclave key 40 is held in protected storage in the security server 24 and the crypt media controller 26. Deo does not overcome this deficiency of Boebert.

Therefore, at least for these reasons, Applicants respectfully submits that claim 10 is patentable over the applied art.

Claims 12-17 are patentable at least for their dependence on claim 10, as well as for the additional features they recite.

Claim 18 recites, *inter alia*, decrypting second data with a decrypting key. As described above with respect to claim 10, Applicants respectfully submit that the applied art does not teach or suggest this feature. As such, Applicants respectfully assert that claim 18 is patentable over the applied art.

Claim 19 is directed to a combination of the data generating apparatus and the data verifying apparatus and recites features similar to those of claims 1 and 10. Claim 19 recites, *inter alia*, a decrypting key generation unit for generating a decrypting key from the second data stored in the first data-for-secondary-checking memory unit, an encrypting key generation unit for generating an encrypting key from the fourth data stored in the second data-for-secondary-checking memory unit, and an encryptor for encrypting the third data generated by the data-for-main-checking generation unit with the encrypting key generated by the encrypting key generation unit.

Again, the Office Action does not identify the data generating apparatus, the data verifying apparatus, the first through fourth data, or how the first through fourth data is encrypted and decrypted. For the data verifying apparatus, the Office Action appears to rely on the rejection of claim 10 on the media key/access vector pair packet as the data to be decrypted. As described above, the media key/access vector pair packet is <u>not</u> decrypted. Furthermore, the Office Action possibly alleges that decryption of the encrypted user's ID or the encrypted request corresponds to the data to be decrypted, as described above, is with the enclave key 40, which is <u>not</u> generated from any data. Thus, Applicants respectfully assert that Boebert does not teach or suggest the decrypting key generation unit for generating a decrypting key recited in claim 19.

For the data generating apparatus, the Office Action appears to rely in the rejection of claim 1 on the user's ID and PIN as the data used to generate an encrypting key, and the media key and the access vector enciphered in the security server 24 as the data to be encrypted.

Therefore, if the same reasoning is applied, Applicants understand that the user's ID and PIN allegedly correspond to the fourth data, and the personal keying device allegedly corresponds to the second data-for-secondary-checking memory unit. Further, Applicants understand that the media key and the access vector allegedly correspond to the third data. Since the media key and the access vector are generated by the key management crypto 70 and the security policy logic 86, as described above, the key management crypto 70 and the security policy logic 86 allegedly correspond to the data-for-main-checking generation unit.

However, claim 19 also recites that the data generating apparatus generates the third data from the first data sent from the data verifying apparatus. Thus, if the third data is the media key and the access vector, the first data should be the data used for generating the media key and the access vector. Claim 19 further recites that the data generating apparatus sends the generated data (e.g., encrypted data) to the data verifying apparatus.

As discussed above, column 13, lines 34-45 describes the generation of the media key and the access vector. According to this section of Boebert, the generation of media key involves "computation, access to stored tables, requests for inputs from authorized individuals, or any combination thereof. Other methods of key generation may also be used." In addition, according to this section of Boebert, the computation of the access vector involves "the intervention of distractive personnel to authorize or deny the granting of certain privileges." However, Boebert does not teach or suggest that such data is sent from the data verifying apparatus (note that, as described above, the Office Action is unclear about what portion of Boebert allegedly corresponds to the data verifying apparatus).

Deo does not overcome these deficiencies of Boebert. As such, at least for these reasons, Applicants respectfully submit that claim 19 is patentable over the applied art.

Claims 20-29 are patentable at least for their dependence on claim 19, as well as for the additional features they recite.

Claim 30 recites, *inter alia*, a first device comprising a first data memory means and an encrypting means, and a second device comprising a second data memory means, a decrypting means and a verifying means. Claim 30 also recites that the first device encrypts prescribed data with the encrypting means on the basis of data stored in the first data memory means, and that if the data is successfully verified, the second device authenticates the identity between the data stored in the first data memory means and the data stored in the second data memory means.

Again, the Office Action does not identify what elements in the applied art allegedly correspond to these claimed features. Since the security server 24 encrypts the media key and the access vector as asserted by the Office Action, Applicants understands that the Office Action alleges that the security server 24 of Boebert corresponds to the first device. However, the Office Action also alleges that the user's ID and PIN are the data used for encryption. As stated by the Office Action, such data is stored in the personal keying device 30. It is clear that the security server 24 and the personal keying device 30 are not one device. Applicants respectfully submit that it is impossible to include the security server 24 and the personal keying device 30 in a single device since Boebert specifically teaches that the user must possess the personal keying device 30.

However, Applicants understand that because the user's ID and PIN are transmitted to the security server 24 and are used for encrypting the media key and the access vector as shown in Fig. 12, there must be a means to temporarily store the user's ID and PIN. With this understanding, Applicants understand that the security server 24 may include a storing means and an encrypting means.

Moreover, because the Office Action states that the crypto media controller 26 decrypts the encrypted media key/access vector pair packet, Applicants understand that the Office Action intends to allege that the crypto media controller 26 corresponds to the second device. However, the crypto media controller 26 does not decrypt the encrypted media key/access vector pair packet 92, and further does not authenticate the identity between the data temporarily stored in the temporary storing means in the security server 24 and the data temporarily stored in the temporary storing means.

At least for these reasons, Applicants respectfully assert that claim 30 is patentable over the applied art.

Claims 31 and 32 are patentable at least for their dependence on claim 30, as well as for the additional features they recite.

In view of the foregoing, it is respectfully submitted that this application is in condition for allowance. Favorable reconsideration and prompt allowance of claims 1, 3-10 and 12-33 are earnestly solicited.

Should the Examiner believe that anything further would be desirable in order to place this application in even better condition for allowance, the Examiner is invited to contact the undersigned at the telephone number set forth below.

Respectfully submitted,

Klifton L. Kime

James A. Oliff
Registration No. 27,075

Klifton L. Kime
Registration No. 42,733

JAO:KLK/aaw

Date: **October 7, 2004**

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

DEPOSIT ACCOUNT USE
AUTHORIZATION
Please grant any extension
necessary for entry;
Charge any fee due to our
Deposit Account No. 15-0461